AMENDMENT TO THE CLAIMS

Claims 1-9, 12, 14, 16-17, 20, 22-32, and 34-36 remain in this application. Claims 1, 9, 12, 17, 23, 24-32, and 34-36 have been amended. Claims 10-11, 13, 15, 18-19, 21, and 33 have been canceled. Thirty new claims have been added.

Listing of Claims:

1. (Currently Amended) A system, comprising:

a local area network (LAN) having at least one host device, the at least one host device having software to perform anti-virus scanning;

a communication module to communicate anti-virus protection information for the at least one host device to ~~the~~ an access module, the anti-virus protection information including status of anti-virus protection of the at least one host device; and

~~an~~ the access module coupled to the LAN to maintain a policy regarding anti-virus protection for the LAN and manage anti-virus protection scanning performed by the at least one host device, the access module to exchange anti-virus protection information with the at least one host device using the communication module of the at least one host device and to deny the at least one host device access to the Internet if the status of the anti-virus protection of the at least one host device is not compliant with the policy.

2. (Original) The system defined in Claim 1 wherein the communication module is part of the at least one host device.

3. (Original) The system defined in Claim 1 wherein the access module sends at

least one command to the at least one host device via the communication module.

4. (Original) The system defined in Claim 3 wherein the at least one command comprises a command selected from a group comprising: a command to request status of the anti-virus protection of the at least on host device, a command to have the at least one host to update the anti-virus protection, a command to uninstall the anti-virus protection, and a command to check a specific file or directory.

5. (Original) The system of claim 1, wherein a system administrator sets a range of compliance for the anti-virus protection policy.

6. (Original) The system of claim 5, wherein the Internet access module denies access to the Internet to the at least one host device if not in the range of compliance.

7. (Original) The system of claim 1, wherein the access module enforces and maintains the anti-virus protection policies for more than one host device.

8. (Original) The system of claim 7, wherein the anti-virus protection policies differ between host devices on the LAN.

9. (Currently Amended) The system of claim 1, wherein the status of the anti-virus protection of the host device ~~communicates~~ includes a version number of the anti-virus protection software on the host device ~~to the access module~~.

10. (canceled)

11. (canceled)

12. (Currently Amended) The system of claim 1, wherein the status of the anti-virus protection of the host device ~~communicates~~ includes a time stamp indicating when the anti-virus protection software was last updated on the host device ~~to the access module~~.

13. (canceled)

14. (Original) The system of claim 1, wherein the access module initiates an update in anti-virus protection for the host-device.

15. (canceled)

16. (Original) The system of claim 1, wherein the host device reports a problem with a virus to the Internet access module.

17. (Currently Amended) The system of claim 1, wherein the access module is one or more of:

a live firewall~~.~~, a proxy server, a router, or a gateway.

18. (canceled)

19. (canceled)

20. (Original) The system of claim 1, wherein the access module is a modem.

21. (canceled)

22. (Original) The system of claim 1, wherein the access module is an application server.

23. (Currently Amended) A method, comprising:

connecting a local area network to an Internet via an Internet access module;

connecting a host device to the Internet via the local area network; and

using the Internet access module to enforce a policy for anti-virus protection on the host device based on the status of anti-virus protection on the host device, wherein the using includes,

denying the host device access to the Internet if the status of the anti-virus protection on the host device is not compliant with the policy.

24. (Currently Amended) The method of claim ~~22~~ 23, further comprising connecting the host device with the Internet access module via an out of band protocol.

25. (Currently Amended) The method of claim ~~23~~ 24, further comprising communicating a version number of the anti-virus protection on the host device to the Internet access module over the out of band protocol.

26. (Currently Amended) The method of claim ~~23~~ 24, further comprising communicating a time stamp indicating when the anti-virus protection was last updated on the host device to the Internet access module over the out of band protocol.

27. (Currently Amended) The method of claim ~~23~~ 24, further comprising initiating an update in anti-virus protection for the host-device over the out of band protocol.

28. (Currently Amended) The method of claim ~~23~~ 24, further comprising encrypting the out of band protocol.

29. (Currently Amended) The method of claim ~~22~~ 23, further comprising connecting more than one host device to the local area network.

30. (Currently Amended) The method of claim ~~28~~ 29, further comprising using the Internet access module enforces and maintains the anti-virus protection policies for more than one host device.

31. (Currently Amended) The method of claim ~~29~~ 30, wherein the anti-virus protection policies differ between host devices.

32. (Currently Amended) The method of claim ~~22~~ 23, further comprising applying a range of compliance for the anti-virus protection policy set by a system administrator.

33. (canceled)

34. (Currently Amended) The method of claim ~~32~~ 33, further comprising:

removing the range of compliance upon notice of a virus alert, and

denying the host device access to the Internet ~~web~~ if the host device does not have the most current ~~version of~~ anti-virus protection.

35. (Currently Amended) The method of claim ~~22~~ 23, further comprising the host device is checked repeatedly to make sure the anti-virus protection is not disabled.

36. (Currently Amended) The method of claim ~~22~~ 23, further comprising reporting a problem with a virus to the Internet access module.

37. (New) A system, comprising:

a local area network (LAN) having at least one host device, the at least one host device having software to perform anti-virus scanning;

a communication module to communicate anti-virus protection information for the at least one host device to an access module, the anti-virus protection information including status of anti-virus protection of the host device; and

the access module coupled to the LAN to maintain a policy regarding anti-virus protection for the LAN and manage anti-virus protection scanning performed by the at least one host device, the access module to exchange anti-virus protection information with the at least one host device using the communication module of the at least one host device and to deny the at least one host device access to the Internet if the status of the anti-virus protection of the at least one host device is not compliant within a range of

compliance for the policy.

38. (New) The system of claim 37, wherein the Internet access module enforces and maintains the anti-virus protection policies for more than one host device; and

wherein the anti-virus protection policies differ between host devices on the LAN.

39. (New) The system of claim 37, wherein the status of the anti-virus protection of the at least one host device includes a version number of the anti-virus protection software on the host device.

40. (New) The system of claim 37, wherein the status of the anti-virus protection of the at least one host device includes a time stamp indicating when the anti-virus protection software was last updated on the at least one host device.

41. (New) The system of claim 37, wherein the Internet access module initiates an update in anti-virus protection for the at least one host device.

42. (New) The system of claim 37, wherein the at least one host device reports a problem with a virus to the Internet access module.

43. (New) The system of claim 37, wherein the Internet access module is one or more of:

a live firewall, a proxy server, a router, a modem, a gateway, or an application server.

44. (New) A system, comprising:

a local area network (LAN) having at least one host device, the at least one host device having software to perform anti-virus scanning;

a communication module to communicate anti-virus protection information for the at least one host device to an access module, the anti-virus protection information including status of anti-virus protection of the host device; and

the access module coupled to the LAN to maintain a policy regarding anti-virus protection for the LAN and manage anti-virus protection scanning performed by the at least one host device, the access module to exchange anti-virus protection information with the at least one host device using the communication module of the at least host device and to deny the at least one host device access to the Internet if the at least one host device does not have anti-virus protection compliant with the policy, wherein compliance with the policy is either a range of compliance or the most up to date anti-virus protection depending on whether there is currently a virus alert.

45. (New) The system of claim 44, wherein the access module enforces and maintains the anti-virus protection policies for more than one host device; and

wherein the anti-virus protection policies differ between host devices on the LAN.

46. (New) The system of claim 44, wherein the status of the anti-virus protection of the at least one host device includes one or more of a version number of the anti-virus protection software on the host device and a time stamp indicating when the anti-virus protection software was last updated on the host device.

47. (New) The system of claim 44, wherein the access module initiates an update in anti-virus protection for the at least one host device.

48. (New) The system of claim 44, wherein the at least one host device reports a problem with a virus to the access module.

49. (New) The system of claim 44, wherein the access module is one or more of:

a live firewall, a proxy server, a router, a modem, a gateway, or an application server.

50. (New) An apparatus comprising:

an Internet access module to be coupled to connect the Internet and a local area network (LAN) including host devices, the Internet access module to receive from the host devices their anti-virus protection status and to deny Internet access to those of the host devices whose anti-virus protection status is not compliant with a corresponding anti-virus protection policy.

51. (New) The apparatus of claim 50, wherein the anti-virus protection policy includes a range of compliance.

52. (New) The apparatus of claim 50, wherein the anti-virus protection policy differs between the host devices on the LAN.

53. (New) The system of claim 50, wherein the status of the anti-virus protection of

at least one of the host devices includes one or more of a version number of the anti-virus protection software on that host device and a time stamp indicating when the anti-virus protection software was last updated on that host device.

54. (New) The system of claim 50, wherein the Internet access module initiates an update in anti-virus protection for at least one of the host devices.

55. (New) The system of claim 50, wherein the Internet access module is one or more of:

a live firewall, a proxy server, a router, a modem, a gateway, or an application server.

56. (New) The system of claim 50, wherein compliance with the anti-virus protection policy is either a range of compliance or the most up to date anti-virus protection depending on whether there is currently a virus alert.

57. (New) A method comprising:

enforcing anti-virus protection in a module providing Internet access to a plurality of host devices belonging to a local area network by performing the following for each of the plurality of host devices repeatedly,

receiving status of the anti-virus protection on the host device,

determining compliance with an anti-virus protection policy based on the anti-virus protection status, and

denying Internet access to the host device if its anti-virus protection status is determined not compliant.

58. (New) The method of claim 57, wherein the determining compliance including determining if the anti-virus protection status is within a range of compliance.

59. (New) The method of claim 57, the performing for each of the plurality of host devices also includes removing the range of compliance upon notices of a virus alert.

60. (New) The method of claim 57, wherein status of the anti-virus protection includes one or more of a version number of the anti-virus protection software on the host device and when the anti-virus protection software was last updated.

61. (New) The method of claim 57, wherein the performing for each of the plurality of host devices also includes initiating an update of the anti-virus protection on the host device.

62. (New) A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

enforcing anti-virus protection in a module providing Internet access to a plurality of host devices belonging to a local area network by performing the following for each of the plurality of host devices repeatedly,

receiving status of the anti-virus protection on the host device,

determining compliance with an anti-virus protection policy based on the anti-virus protection status, and

denying Internet access to the host device if its anti-virus protection status is determined not compliant.

63. (New) The machine-readable medium of claim 62, wherein the determining compliance including determining if the anti-virus protection status is within a range of compliance.

64. (New) The machine-readable medium of claim 62, the performing for each of the plurality of host devices also includes removing the range of compliance upon notices of a virus alert.

65. (New) The machine-readable medium of claim 62, wherein status of the anti-virus protection includes one or more of a version number of the anti-virus protection software on the host device and when the anti-virus protection software was last updated.

66. (New) The machine-readable medium of claim 62, wherein the performing for each of the plurality of host devices also includes initiating an update of the anti-virus protection on the host device.